



Hands-On Hardware Hacking and Reverse Engineering Techniques

Document Revision: 1.2

Last updated: September 19, 2008

(Times for each section are approximate)

1. Introduction to Hardware Hacking (1 hour)

- 1.1. Hacker v. Attacker
- 1.2. A Brief History of Hardware Hacking
- 1.3. What is Hardware Hacking and Reverse Engineering?
- 1.4. Legal Issues
- 1.5. Challenges and Trends
- 1.6. Hardware Hacking Methodology: How to Approach the Problem
- 1.7. Examples of Interesting Hacks

2. Tools of the Warranty Voiding Trade (0.5 hours)

- 2.1. Tools Provided in this Course
- 2.2. The Essential Tools
- 2.3. Basic Hardware Hacking
- 2.4. Advanced Projects and Reverse Engineering

3. Soldering and Desoldering (1.5 hours)

- 3.1. Hands-on: Soldering a resistor to the circuit board
- 3.2. Hands-on: Desoldering a connection using the solder sucker
- 3.3. Hands-on: SMD removal using ChipQuik

4. Electrical Engineering Fundamentals (2 hours)

- 4.1. Bits, Bytes, and Nibbles
- 4.2. Voltage, Current, and Resistance
 - 4.2.1. Voltage
 - 4.2.2. Current
 - 4.2.3. Power
 - 4.2.4. Direct Current (DC) and Alternating Current (AC)

- 4.2.5. Resistance
- 4.2.6. Ohm's Law
- 4.3. Basic Device Theory
 - 4.3.1. Switches
 - 4.3.2. Resistors and Potentiometers
 - 4.3.3. Capacitors
 - 4.3.4. Inductors
 - 4.3.5. Diodes and LEDs
 - 4.3.6. Transistors
 - 4.3.7. Integrated Circuits (ICs)
 - 4.3.8. Digital Logic
 - 4.3.9. Microcontrollers
 - 4.3.10. Memory (RAM, ROM, EEPROM, Flash)
 - 4.3.11. Programmable Logic (ASICs, FPGAs)

5. Reading and Drawing Schematics (0.25 hours)

- 5.1. Reading Schematics
- 5.2. Common Schematic Symbols
- 5.3. Drawing Schematics

6. Building and Modifying Circuits (0.75 hours)

- 6.1. Prototyping and Breadboarding
- 6.2. Custom Printed Circuit Boards
- 6.3. Modifying Circuit Boards
 - 6.3.1. Hands-on: Cutting a trace on the circuit board
- 6.4. Common Engineering Mistakes

7. A Look at Embedded Security (0.5 hours)

- 7.1. General Security Concepts
- 7.2. Hardware Security Myths and Common Problems
- 7.3. Types of Attacks and Attackers
- 7.4. Goals of an Attack
- 7.5. Anti-Tamper Mechanisms
- 7.6. Ramifications of Secure Hardware

8. Cracking the Case: Opening Product Housings (0.25 hours)

- 8.1. The Basics
- 8.2. Step-by-Step
- 8.3. Tips
- 8.4. Security Bits and One-Way Screws

8.5. Epoxy Encapsulation Removal

9. Reverse Engineering (3 hours)

9.1. Component Identification and Package Marking Information

9.2. Finding Data Sheets

9.3. Probing Boards and Tracing Signals

9.3.1. Design-for-Manufacturability and Test

9.3.2. Probing Boards

9.3.3. Hands-on: Experiments with the Multimeter

9.3.4. Hands-on: Learning to use the Parallax USB Oscilloscope

10. Memory and Programmable Logic (1 hour)

10.1. General Issues

10.2. Hands-On: Read Serial EEPROM memory contents with a device programmer

11. External Interfaces (0.5 hours)

11.1. General External Interfaces

11.2. JTAG (IEEE 1149.1)

11.3. Backdoors

12. Advanced Hardware Hacking Techniques (0.5 hours)

12.1. Emissions and Side-Channel Attacks

12.2. Chip Decapping and Die Analysis

13. Grand Idea Studio's "Hardware Hacking Challenge" (remaining available time)

14. Resources

14.1. Books and Magazines

14.1.1. General Electrical Engineering

14.1.2. Hardware Hacking

14.1.3. Hobbyist and Robotics

14.2. Web Sites

14.2.1. Electrical Engineering

14.2.2. Hardware Hacking

14.3. Other Resources

14.4. Distributors

14.4.1. Electrical Engineering

14.4.2. Tools and General Hardware